CLAIMS:

1. An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorised party or entity to a computer system or network, the intrusion detection system comprising means for monitoring activity relative to said computer system or network, means for receiving and storing one or more general rules, each of said general rules being representative of characteristics associated with plurality of specific instances of intrusion or attempted intrusion, and matching means for receiving data relating to activity relative to said computer system or network from said monitoring means and for comparing, in a semantic manner, sets of actions forming said activity against said one or more general rules to identify an intrusion or attempted intrusion.

2. An intrusion detection system according to claim 1, wherein said one or more general rules forms a knowledge base of the system, and wherein the system comprises means for automatically generating and storing in said knowledge base a new general rule representative of characteristics associated with specific instances of intrusion or attempted intrusion not previously taken into account.

3. An intrusion detection system according to claim 2, wherein said means for automatically generating and storing a new general rule comprises inductive logic programming means.

4. An intrusion detection system according to any one of the preceding claims, wherein said one or more general rules is or are represented in a logic programming language.

5. An intrusion detection system according to claim 3, wherein inductive logic programming techniques are applied by the system to an attack an intrusion or attempted intrusion.

6. An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorised party or entity to a computer system or network, the intrusion detection system comprising means for monitoring activity relative to said computer system or network, means for initially receiving and storing a knowledge base comprising one or more general rules, each of said general rules being representative of characteristics associated with a plurality of specific instances of intrusion or attempted intrusion, and means for automatically generating

and storing in said knowledge base (after said knowledge base has been initially stored) new general rules representative of characteristics associated with specific instances of intrusion or attempted intrusion not previously taken into account.

7. An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorised party or entity to a computer system or network, the intrusion detection system comprising means for monitoring activity relative to said computer system or network, means for initially receiving and storing in a knowledge base data representative of characteristics associated with one or more specific instances or classes of intrusion or attempted intrusion, matching means for receiving data relating to activity relative to said computer system or network from said monitoring means and for comparing sets of actions forming said activity against said stored data to identify an intrusion or attempted intrusion, and inductive logic programming means for updating said stored data to take into account characteristics of further instances or classes of intrusion or attempted intrusion occurring after said knowledge base has been initially received and stored.

8. An intrusion detection system substantially as herein described with reference to the accompanying drawings.